Technical Disclosure Commons

Defensive Publications Series

June 07, 2017

Determining User Location Using IP Address and Historical Device Locations

Oliver Voggenreiter

Ankit Gupta

Determining User Location Using IP Address and Historical Device Locations

Responses to user searches and other queries are often most relevant when tied to the user's location. Thus, when a user interacts with online services, it is often useful to provide location information to the service in order to improve the quality of service or ensure correct handling of a user's data or access. When the user provides a precise location signal (e.g., from an on-device GPS signal), the service can employ this signal to provide a better experience associated with the user's location. However, when no such precise signal is present, the service will be restricted in the information available to determine a predicted user location. Even if historically collected locations of the user exist, these may be spread across a relatively large area (or areas). Such location information may represent a very coarse approximation of the user's location, for instance representing their home, work, points of interest, travel route, vacations spots, etc.

Aspects of the technology focus on providing an estimation of the user's location in the absence of a precise location signal, as precisely as possible. In particular, historically collected locations of a user are segmented by their associated IP address/subnet (the IP address/subnet used at the time of the collection of said locations). This provides focused groups of locations that represent the estimated location(s) of a user while on various IP addresses/subnets. The IP address/subnet can represent not only a virtual location, but often correlates with a physical location.

For instance, when a user is on a mobile carrier signal (e.g., as part of a 4G LTE network), the user's communication device will be using that carrier's assigned IP address when connecting to or requesting services online. A different IP address would be used when the user is connected to his or her network at home (WiFi) or his place of work (internal corporate

network or VPN) or other places of interest (e.g., public WiFi at cafes, airports, transport networks, etc.). When the user's location is matched to a unique identification (e.g., a browser cookie) and an IP address, this provides a more precise estimate of the user's likely location. Once such estimates have been collected by the system, they may be used to approximate the user's location when they make a request to the service without a precise location (or any location signal at all) in order to maintain a higher quality of service.

In practice, a personalized location module (PLM) may be implemented as part of a location-based service or system. It may be associated with one or more cookies linked with a search event. The PLM is used to infer locations from search events for individual users. The inference approach is arranged in such a way that it may find one or two relevant locations per user. For instance, this may enable finding home and/or work locations of users (as long as enough search events are known).

One aspect adds a user's IP address / subnet as part of the key on which location information is computed. In other words, instead of computing a location for all events for a given cookie, the location may be determined for a cookie and IP subnet pair in combination. It is important to note that different IP subnets for a single user likely correspond to different locations and usage patterns. For example, this may include a carrier IP of a mobile device while on the go, a consumer ISP address while connected to the WiFi at home, and a corporate ISP address of an employer while connected to the WiFi at work. By making the IP address subnet a part of the inference key, the system can *a priori* distinguish these different situations. This is more efficient and accurate than *a posteriori* attempting to find different peaks in the total point cloud of user location information. Using information about the user's current connection to the Internet will make the system more accurate and robust.

The size of subnets on which the system may key should be large enough to allow for dynamic IP assignments of the user's home ISP, while still distinguishing different ISPs and home ISPs from carrier IPs (where feasible). Typically, IP ranges from different ISPs are very different, so the subnets can be chosen generously. According to one example, the system may use /16 for IPv4 and /32 for IPv6. Nonetheless, other choices (e. g., /24 and /48) are also possible.

According to another aspect of the technology, the system may have a fallback location keyed only on the user, based on pre-stored information. This could be used if a user is seen on an unknown IP subnet (or on more subnets than the system has storage capacity for). This may be inferred with the "old" logic of using information associated with this user, or only from events that originate from a subnet not included in the keys. In this situation, the process could use only the user cookie as a key. All IP-keyed locations would be stored in the value. Otherwise, the system would need to do two look-ups (with and without IP information), but those could possibly be done with a single request.

However, instead of the fallback approach, using two or three IP keys for home/work/carrier would provide coverage most of the time. For other situations, it may not be feasible to obtain a useful location inference.

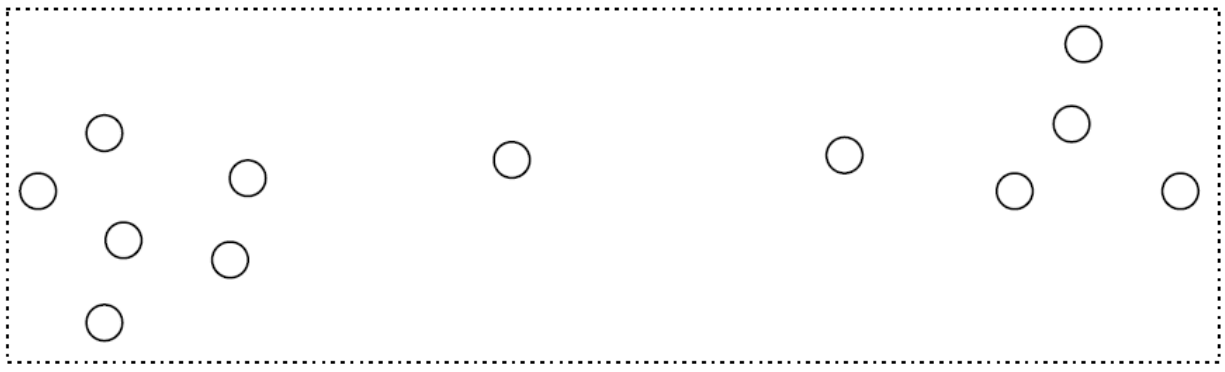
With keying on IP information, the system may simplify the inference process to always just try to find the center of a point cloud of locations. Since one technique uses the IP subnet to distinguish common "cases" for a user, there will not be that much need to find more than one location. Ideally, home and work (or other common locations) could be distinguished already by using known IP information. This is, however, not guaranteed. Some users might not actually

log into WiFi at work (or even have the ability to do so), or there might be multiple important places visited from their carrier IP.

In one scenario, having two keys makes sense to cover the home and work scenarios. But some scenarios are different. How often other scenarios occur may warrant a third key or even more keys. But if the user is always on carrier IPs, there is no point in having any IP keys. If the user connects to his/her Gym, or other places they regularly visit, they could benefit from more than two keys. Thus, the system should be flexible to accommodate these different scenarios.

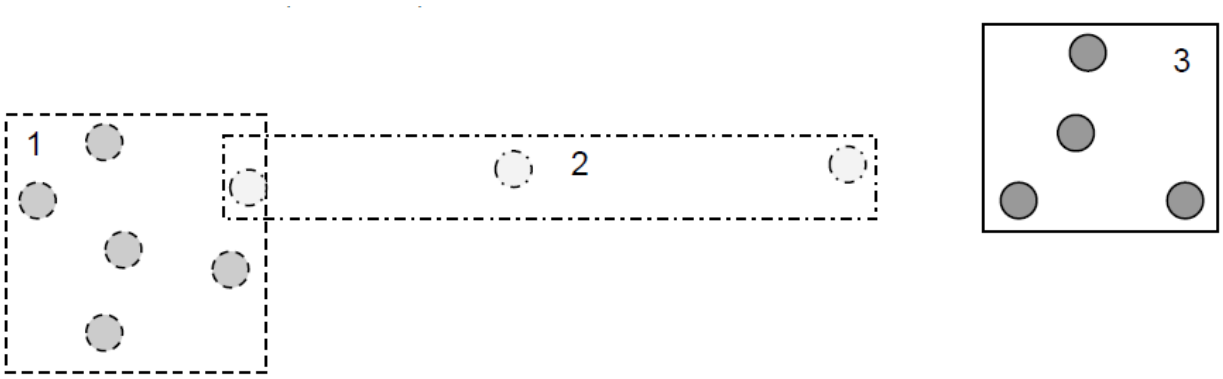
Another factor is the freshness of key selection. For instance, what if a user is visiting a new city and uses hotel WiFi for several days. The system can evaluate the situation based on the timing and/or other factors to determine whether to add the hotel WiFi as an IP key.

The following provides two graphics that depict the selection of an approximation of a user's location. The first image gives a general historical location model, where each circle within the dotted rectangle represents an acquired location signal for a user. The rectangle provides a general location.



In this first case (the general model), all of the information is taken into consideration and a user is likely to be located anywhere within the bounds of the dotted rectangle (or even outside of it). However, this may not give a useful location, which means that any search query or other results might be of little to no relevance.

The second case, as shown below, provides much more useful location results.



According to aspects of the technology, the IP address segmented model would be able to create multiple approximations depending on the number of IP addresses (which are indicated by different shades of gray in the image above) present in the historical location information for the user. These locations may provide smaller more refined approximations of the user's location, in this example by the three small rectangles. The system would provide the information of whether the user is not in any of them (when the IP of the user does not match any model).

Thus, it can be seen that the system may look at many different locations and an extended timeframe, and segment the locations by IP address and user information (e.g., cookies). The system may process the information in two phases. In the first phase, possible locations are preprocessed according to historical information with IP addresses. Then in the second, live stage, the system could look at the current IP address and cookie or other information in relation to the historical data to assess the user's likely location. Then location-relevant search results may be provided back to the user in real time. By using the serving-time IP address, the system thus provides a more fine-grained estimate of the user's location than conventional approaches.

Aspects of the technology may be implemented using one or more computing devices such as a server or cloud computing system. These computing devices each have at least one processor, which can be any conventional processor, such as a commercially available CPU.

Alternatively, the processor(s) can be dedicated components such as an application specific integrated circuit ("ASIC") or other hardware-based processor.

The processors, computer, computing device, or memory of the system can comprise multiple processors, computers, computing devices, or memories that may or may not be stored within the same physical housing. For example, the memory can be a hard drive or other storage media located in housings different from that of the computing devices. Although some functions described herein may take place on a single computing device having a single processor, various aspects of the subject matter described herein can be implemented by a plurality of computing devices, for example, communicating information over a network.

Each computing devices can be at different nodes of a network and capable of directly and indirectly communicating with other nodes of network. A typical system can include a large number of connected computing devices, with each different computing device being at a different node of the network. The network and intervening nodes described herein can be interconnected using various protocols and systems, such that the network can be part of the Internet, World Wide Web, specific intranets, wide area networks, or local networks. The network can utilize standard communications protocols, such as Ethernet, WiFi and HTTP, protocols that are proprietary to one or more companies, and various combinations of the foregoing. Although certain advantages are obtained when information is transmitted or received as noted above, other aspects of the subject matter described herein are not limited to any particular manner of transmission of information.

As an example, each computing device may include web servers capable of communicating with a storage system as well as with client computing devices via the network.

For example, one or more of server computing devices may use network to transmit and present information to a user on a display.

Although the client computing devices may each comprise a full-sized personal computing device, they may alternatively comprise mobile computing devices capable of wirelessly exchanging data with a server over a network such as the Internet. By way of example only, the client computing devices may be a mobile phone or a device such as a wireless-enabled PDA, a tablet PC, or a netbook that is capable of obtaining information via the Internet. In another example, client computing device may be a head-mounted or wearable computing system. As an example the user may input information using a small keyboard, a keypad, microphone, using visual signals with a camera, or a touch screen.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

Abstract

An enhanced location system uses both IP address (e.g., subnet) and user ID information (e.g., cookie) to differentiate, in view of historical information, a most likely location of a user.

Using the IP information a part of a location inference key, the system quickly and easily filters the historical information to identify the location. Having the location enables the system to provide, in real time, location relevant answer or other results responsive to a user's query.